Chapter 7: Accessing Kerberized Machines (Community-Supported Methods)

In this chapter we discuss accessing systems in the FNAL.GOV realm from UNIX, Windows and Macintosh machines using programs or operating systems not supported by the Computing Division.

Very important note: Any time you're about to enter your Kerberos password, first verify that you're using the host's directly-connected keyboard or using an encrypted connection! Otherwise you risk exposing your password. See Chapter 11: *Encrypted vs. Unencrypted Connections* for information.

7.1 Logging In Through Kerberized Exceed 7 Software from Windows

7.1.1 Telnet Connections

You should create one secure telnet profile for each Kerberized host you wish to access, according to the instructions in section 21.5 *Configuring the Exceed 7 Telnet Application*. To authenticate:

- using the **Leash32** utility, navigate to **START** > **PROGRAMS** > **KERBEROS UTILITIES** > **LEASH32**. Select **GET TICKET** on the **ACTION** menu.

  You will be required to enter your Kerberos password. Ignore the CRYPTOCard prompt that may follow (press **CANCEL**). You ticket will appear in the **Leash32** window. Click on the Windows Explorer-style plus signs (+) to get details.

- using the command prompt, type **`kinit -5`** to request a ticket.

  You will be required to enter your Kerberos password. Ignore the CRYPTOCard prompt that may follow (just press **ENTER**). To verify the ticket and its flags, either bring up the **Leash32** window, or type **`klist -f`** at the command prompt.

  You can request a renewable ticket at the command prompt by using the **`-r`** option (see section 9.2.5 *Renewing Tickets*). Your AFS token will have a lifetime equal to the renewable lifetime of the Kerberos ticket.

To connect:

1) Start the Exceed 7 telnet program. Navigate to **START** > **PROGRAMS** > **HUMMINGBIRD CONNECTIVITY V7.0** > **HOSTEXPLORER** > **TELNET**.

2) On the **OPEN SESSION** window, with the desired telnet profile selected, the target host name or IP address should appear in the Host Name window. To connect, click on the **CONNECT** button. If you've preauthenticated, you should get right in without having to provide your Kerberos password.

3) The **LEASH32** window should now show your host connection in addition to the kerberos ticket.

7.1.2 FTP Connections

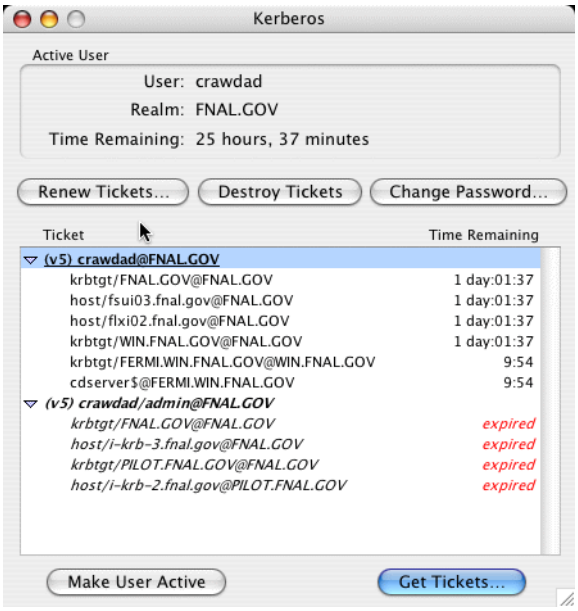
Exceed 7 does not provide a Kerberized FTP client. Furthermore, you cannot connect using your CRYPTOCard (as you may for WRQ® FTP, described in section 4.6.3 *Run an FTP Session to Kerberized Host*), since the Exceed 7 FTP client stores your password, and doesn't let you enter it each time you connect. Choose a different product! Suggestions: WRQ®, FileZilla, AFS Windows Client (for remote hosts using AFS).

7.2 Logging In from a Macintosh

Here we assume you are running the **MIT Kerberos** OS X 10 software for Macintosh as described in Chapter 23: *Installing and Configuring MIT Kerberos on a Macintosh System*.

There are two ways to authenticate to Kerberos on the Macintosh:

- Open a terminal window and use the command line **`kinit`** as you would on a Unix system. If you are logged into the machine under a username that's the same as your principal, just run **`kinit`** from your home directory, and Kerberos will pick the right principal for you. Otherwise you'll have to give your principal in the command: **`kinit [principal]`**.
- If you've installed the "Extras", go to the /Applications/Utilities folder and select Kerberos. You have to tell the Kerberos GUI what your Kerberos principal is. Click "Get Tickets".



You should see a ticket appear. Now you can invoke your **telnet** or **ssh** client and connect to one or more strengthened hosts without having to provide your password again. You have to tell telnet or ssh the name of the remote account you want to log in to, unless it's the same as the local account name (regardless of what your Kerberos principal is).